## CHAPTER 4 – INFORMATION TECHNOLOGY

## ARTICLE 45 — INFORMATION SECURITY

*Revised May 20, 2013*

### 49020.1 Policy

It is the policy of the California Department of Corrections and Rehabilitation (CDCR) to protect against the unauthorized modification, deletion, or disclosure of information included in agency files and databases. The Department regards its information assets, including data processing capabilities and automated files, to be essential resources. The Department shall assume full responsibility for ensuring the security and integrity of its information resources.

### 49020.2 Purpose

The purpose of this Policy is to establish and maintain a standard of due care to prevent misuse or loss of Department information assets. This policy establishes internal policies and procedures that:

- Establish and maintain management and staff accountability for the protection of departmental information assets.
- Establish and maintain processes for the analysis of risks associated with departmental information assets.
- Establish and maintain cost-effective risk management processes intended to preserve the Department's ability to meet program objectives in the event of the unavailability, loss, or misuse of information assets.
- Protect departmental employees who are authorized to access the Department's information assets from temptation, coercion, and threat.
- Establish agreements with state and non-state entities to cover, at a minimum, the following:
    - Appropriate levels of confidentiality for the data based on data classification (see State Administrative Manual [SAM], § 5320.5).
    - Standards for transmission and storage of the data, if applicable (see SAM § 5310).
    - Agreement to comply with all state policy and law regarding use of information resources and data.
    - Signed confidentiality statements.
    - Agreements to apply security patches and upgrades, and keep virus software up-to-date on all systems on which data may be used.
    - Agreements to notify the information owners promptly if a security incident involving the data occurs.
- Establish appropriate policies and procedures to protect and secure IT infrastructure.
- Require that if a data file is downloaded to a mobile device or desktop computer from another computer system, the specifications for information integrity and security which have been established for the original data file must be applied in the new environment (SAM § 5310).
- Require encryption, or equally effective measures, for all personal, sensitive, or confidential information that is stored on portable electronic storage media (including, but not limited to, CDs and thumb drives) and on portable computing devices (including, but not limited to, laptop and notebook computers). This policy does not apply to mainframe and server tapes. (See SAM Section 5345.2).

### 49020.3 Statutory References Concerning the Confidentiality and Security of Information within CDCR

SAM § 5300.3 requires the Secretary/Director of each State agency that uses, receives, or provides services to designate an Agency Information Security Officer (ISO) who shall be responsible for implementing State policies and standards regarding the confidentiality and security of information within the Department. These policies and standards shall include, but are not limited to, strict controls to prevent unauthorized access of data maintained in computer files, program documentation, data processing systems, data files, and

data processing equipment located physically in the Department and to establish guidelines for the dissemination of information under the control of California State agencies as found in the State Constitution, in statutes, and in administrative policies:

- Article 1, Section 1, of the Constitution of the State of California defines pursuing and obtaining privacy as an inalienable right.
- The Information Practices Act of 1977 (Civil Code [CC], § 1798, et seq.), places specific requirements on State agencies in the collection, use, maintenance, and dissemination of information relating to individuals.
- The California Public Records Act (Government Code [GC], §§ 6250-6265), provides for the inspection of public records.
- The State Records Management Act (GC, §§ 14740-14770) provides for the application of management methods to create, use, maintain, retain, preserve, and dispose of State records, including the determination of records essential to the continuation of State government in the event of a major disaster. SAM, §§ 1601-1699 contains administrative policies to implement provisions of this law.
- The California Penal Code (PC), § 502 covers the following offenses:
  - Manipulating data, a computer system, or computer network to devise or execute a fraud.
  - Knowingly accessing and, without permission, taking copies or using any data from a computer or taking any supporting documentation, internal or external, to a computer.
  - Theft of computer services.
  - Knowingly accessing and without permission, damaging data, software, or applications/programs, internal or external, to a computer.
  - Disrupting or denying computer services to an authorized user.
- The California PC § 11142 provides that, "Any person authorized by law to receive a record or information obtained from a record who knowingly furnishes the record or information to a person who is not authorized by law to receive the record or information is guilty of a misdemeanor."
- The Federal Copyright Act of 1976 provides for the prosecution of persons guilty of the theft of computer programs.

### 49020.4 Departmental Approach to Information Security

The departmental approach to information security consists of the following components:

- Assigned management responsibilities for IT risk management. See SAM § 5315.
- Provisions for the integrity and security of automated and paper information, produced or used in the course of CDCR operations. See SAM § 5310 through 5350.
- Provisions for the security of IT facilities, software, and equipment utilized for automation. See SAM § 5330.
- Establishment and maintenance of an IT risk management program, including a risk analysis process. See SAM § 5305.
- Establishment and maintenance of an agency Disaster Recovery Plan. See SAM § 5355.
- A security and ongoing privacy program, including an annual training component for all employees and contractors. Refer to GC 11019.9 and CC 1798.
- Compliance with state audit requirements relating to the integrity of information assets. See SAM § 20000 et seq.
- Policies to ensure that information security and information privacy are incorporated at each phase of the Information Systems Development Life Cycle.
- Risk assessments in accordance with SAM, § 5305.1 to ascertain the threats and vulnerabilities that impact the CDCR's information assets and implement appropriate mitigations.
- Information security training for employees who use information assets in the course of their assigned duties to ensure awareness and understanding of the Department's policies.
- Coordination of information security audits for compliance with security policies.

- Reporting of deficiencies for noncompliance with the CDCR security policies for management's corrective action.
- Reporting violations of this policy to the hiring authority of the employee alleged to have committed the act or the Office of Internal Affairs (OIA), when appropriate.
- Adherence to requirements established in SAM, § 5300.3.
- Periodic review of security policies for changes that may be necessary as a result of technology evolution or changes in Department operations.

This policy includes, but is not limited to, the following information assets:

- All categories of automated information including, but not limited to, records, files, and data bases.
- IT facilities, software, and equipment (including personal computer systems) owned or leased by the CDCR.

### 49020.5 Roles and Responsibilities

The Department has established the necessary policies, procedures, practices, and controls to protect information assets from accidental or intentional disclosure, destruction, or modification, and to comply with all applicable State and federal privacy acts. Information assets covered by this Article include, but are not limited to:

- All categories of automated information including, but not limited to, records, files, and data bases.
- IT facilities, software, and equipment (including personal computer systems) owned or leased by the CDCR.

The following is a description of the organizational responsibilities for administering this program:

**Secretary**

The Secretary has the ultimate responsibility for ensuring a risk management program is established that:

- Assigns management responsibilities for IT risk management.
- Provides for the integrity and security of automated and paper information, produced or used in the course of agency operations.
- Complies with state and audit requirements relating to the integrity of information assets.

**Director of Enterprise Information Services (EIS)**

The Director of EIS has the delegated responsibility for establishing and maintaining an information security program within the Department. It is the responsibility of the Director of EIS to assure that information assets are protected from the effects of damage and destruction, as well as from unauthorized or accidental modification, access, or disclosure. Specifically, the Director of EIS is responsible for ensuring:

- Enforcement of State-level security policies.
- Establishment and maintenance of internal policies that provide for the security of IT facilities, software and equipment, and the integrity and security of the agency's automated information.
- Department compliance with reporting requirements related to security issues.
- Appointment of a qualified AISO.
- The participation of management during the planning, development, modification, and implementation of security policies and procedures.

**Agency Information Security Officer (AISO)**

SAM, § 5315.1 requires that each agency designate an AISO. Additionally, to avoid conflicts of interest, the following restrictions shall apply to the AISO:

- The AISO shall not have direct responsibility for information processing.
- The AISO shall not have direct responsibility for access management functions.
- The AISO shall not have direct responsibility for any departmental computer-based systems.

- The AISO shall not have any special allegiance or bias toward a particular program or organization.
- The AISO will have direct responsibility for the CDCR Information Security Office.
- The AISO will report allegations of misconduct or criminal activity to OIA and assist with investigations as necessary.

The AISO is responsible for overseeing Agency policies and procedures designed to protect its information assets. In accordance with State policy, the AISO shall be accountable to the Secretary with respect to the following responsibilities:

- Implementation of necessary procedures to ensure the establishment and maintenance of a security program.
- Establishment of security policies and procedures designed to protect information assets.
- Identification of confidential and sensitive information and critical applications.
- Identification of vulnerabilities that may cause inappropriate or accidental access, destruction or disclosure of information, and the establishment of security controls necessary to eliminate or minimize their potential effects.
- Establishment of procedures necessary to monitor and ensure the compliance of established security and risk management policies and procedures.
- Coordination with internal auditors to define their roles in automated information system planning, development, implementation, operations, and modifications relative to security.
- Coordination with the applicable data center's Information Security Officer or staff on matters related to the planning, development, implementation, or modification of information security policies and procedures that affect the Department.
- Acquisition of appropriate security equipment and software.
- Establishment of procedures to comply with control agency reporting requirements.
- Development and maintenance of controls and safeguards to control user access to information.
- Establishment of mechanisms to assure that CDCR staff (with particular emphasis on the owners, users, and custodians of information) are educated and aware of their roles and responsibilities relative to information security.
- Establishment of training programs for CDCR employees related to information security.

**EIS Technical Management**

Department technical management has the following responsibilities relative to the Department's information security program:

- Ensuring that management, the Information Security Office, assigned owners, custodians, and users are provided the necessary technical support services with which to define and select cost effective security controls, policies, and procedures.
- Ensuring the implementation of security controls and procedures as defined by the owners of information.
- Ensuring the implementation of system controls necessary to identify actual or attempted violations of security policies or procedures.
- Ensuring that the owners of information and the Information Security Office are notified of any actual or attempted violations of security policies and procedures.

**Program Management**

Department program managers have the following responsibilities in relation to the Department's security program:

- Establishing the procedures necessary to comply with State information security policy in relation to ownership, user, and if appropriate, custodian of information responsibilities.
- Ensuring that State program policies and requirements are identified relative to security requirements.

- Ensuring the proper data classification of automated information for which the program is assigned ownership responsibility.
- Ensuring the participation of the Information Security Office and technical staff in identifying and selecting appropriate and cost-effective security controls and procedures, and to protect information assets.
- Ensuring that appropriate security requirements for user access to automated information are defined for files or data bases for which the program is assigned ownership responsibility.
- Ensuring the proper planning, development, and establishment of security policies and procedures for files or data bases for which the program has ownership responsibility, and for physical devices assigned to and located in the program area(s).
- Ensuring that custodians of program information are provided the appropriate direction to implement the security controls and procedures that have been defined.
- Ensuring that procedures are established to comply with control agency reporting requirements.

**Program Personnel and Users**

Program personnel have the following security responsibilities:

- Implementing and monitoring data quality assurance functions to ensure the integrity of data for which the program is assigned ownership responsibility.
- Complying with applicable federal, State, and Department security policies and procedures.
- Complying with applicable federal and State statutes.
- Identifying security vulnerabilities and informing program management and the Information Security Office of those vulnerabilities.
- Ensuring that management, the Information Security Office, and assigned owners, custodians, and other users are provided the necessary technical support services with which to define and select cost-effective security controls, policies, and procedures.
- Ensuring the implementation of security controls and procedures as defined by the owners of information.
- Ensuring the implementation of system controls necessary to identify actual or attempted violations of security policies or procedures.
- Ensuring that the owners of information and the Information Security Office are notified of any actual or attempted violations of security policies and procedures.

**Data Owners**

The owners of information are responsible for classifying the information, defining precautions for its integrity, disposing of the information, defining initial levels of access needed, filing security incident reports, securing signed security agreements, and forwarding them to the Data Custodian, and identifying the level of acceptable risk.

**Data Custodians**

The custodians of information, including the Office of Technology Services (OTech) Data Center, are responsible for complying with applicable laws, policies and procedures established by the owner and the AISO, advising the owner and the AISO of any threats to the information, and notifying the owners and the AISO of any violations of security policies, practices, and procedures.

In addition, the data custodians for an information system have the following access management responsibilities:

- Access Authorization - The granting of permission to execute a set of operations in the system. Access privileges shall be allocated to users on a need-to-use basis, with the minimum required privileges required for their functional role.

- Access Control - Enabling the performance of tasks by hardware, software, and administrative controls that would have the effect of monitoring a system's operation, ensuring data recovery, performing user identification, and granting access to users.
- Accountability - The work necessary to set up the ability to trace violations or attempted violations of system security to the individual(s) responsible.

**Information Security Coordinators**

Every organizational entity that uses computer systems, or uses computer applications shall designate an Information Security Coordinator (ISC) for each site maintained by that entity. The designated ISC shall be responsible for ensuring that applicable CDCR policies and procedures are followed, and shall act as the security liaison to the Information Security Office. The CDCR Information Security Office will serve as the ISC for EIS staff.

A procedure shall be developed by each of these organizational entities, subject to approval by the AISO. The procedure shall be constrained as follows:

- The designation of an ISC for the decentralized or control entity shall be in writing and shall identify the name, work address, and telephone number of the ISC.
- The AISO shall maintain a file of all current and past designated ISCs.
- The designated ISC shall be aware that they are the designated ISC and the responsibility that the designation entails.
- The designated ISC shall ensure compliance with information security policies and procedures, and with any security guidelines issued by the owners of decentralized automated systems.

### 49020. 6 CDCR Information Asset Protection

CDCR shall provide for the integrity and security of its information assets by identifying all automated files and databases for which CDCR has ownership responsibility, and ensuring that responsibility for each automated file or database is defined with respect to the following:

- Owners of the information within CDCR.
- Custodians of the information.
- Users of the information.
- Classification of the information to ensure that each automated file or database is identified as to its information class in accordance with law and administrative policy.

### 49020.6.1 Information Security Ownership/Authority

An owner of any CDCR information shall be the approval authority for all requests for access to such information under his or her control. Approval authority may be delegated to a designated representative. The owner has an obligation to restrict access to the specific information to instances that are necessary and sufficient to meet the demonstrated need or right of the requestor. The owner shall consult with EIS to determine the most appropriate on-line access mechanisms for a specific request, keeping in mind that EIS is obligated to restrict the mechanisms to those that are necessary and sufficient to meet the requestor's need for, or right to, such information.

The owner is ultimately responsible for the integrity of the entrusted information. This responsibility requires that the owner have control over who can access, modify, disclose, or destroy information. The owner shall exercise the responsibility to communicate information security requirements to all appropriate personnel, and to make use of all available security features. Additionally, the owner shall determine that implemented security measures are adequate to meet the requirements of the application, and ensure that an employee's access authority is removed immediately upon separation or change of duties such that access is no longer necessary.

### 49020.6.2 Classification of Information

CDCR's records, automated files, and databases are essential public resources that must be given appropriate protections from unauthorized use, access, disclosure, modification, loss, or deletion. The discovery and classification of CDCR Information Assets is a continuing endeavor and requires the ongoing support of information owners and other stakeholders.

- The EIS Enterprise Architecture organization is responsible for maintaining and facilitating the processes and procedures for enterprise governance of CDCR Information Assets and engaging Information Owners and Stakeholders for Information Security Classification decision-making and governance.
- Information Owners are responsible for reviewing and classifying information, solely or with others, for information they own or share ownership of, and for participating in the CDCR Information Governance process; the final ruling for Security Classification decisions rests with the Information Owners.
- Stakeholders are responsible for raising Information security concerns with respect to Information Security Classification and ensuring information is treated appropriately based on duly made classification decisions.
- All users of CDCR Information are responsible for protecting CDCR Information under their control or influence from unauthorized use, access, disclosure, modification, loss, or deletion, including notifying appropriate CDCR authorities when vulnerabilities to CDCR Information is noticed or when Security Classifications or protections for CDCR Information appear inadequate.

CDCR will classify each record, file, and database using the following classification structure:

- Public Information – information maintained by CDCR that is not exempt from disclosure under the provisions of the California Public Records Act (GC §§ 6250-6265) or other applicable state or federal laws (SAM § 5320.5).
- Confidential Information – information maintained by CDCR that is exempt from disclosure under the provisions of the California Public Records Act (GC §§ 6250-6265) or other applicable state or federal laws (SAM § 5320.5).
- High Risk Confidential Information (HRCI) - Non-public information that if disclosed could result in a significant harm (including financial, legal, risk to life and safety or reputational damage) to the CDCR or individual(s) if compromised through alteration, corruption, loss, misuse, or unauthorized disclosure. Examples of HRCI include, but are not limited to, information such as the following:
  - Personally identifiable information such as person's name in conjunction with the person's social security, credit or debit card information, individual financial account, driver's license number, state ID number, or passport number, or a name in conjunction with biometric information;
  - Personal health information such as any information about health status, provisions of health care, or payment for health care information as protected under the Health Insurance and Portability Act of 1996;
  - Correctional Offender Record Information as defined in California PC §§ 13100-13104;
  - All IT infrastructure information that would reveal vulnerabilities to, or otherwise increase the potential for an attack on, an information technology system of a public agency, including but not limited to firewall and router configurations, server names, IP addresses, and other system configurations;
  - Any Document which contains information identifying any Confidential Informant, or confidential information provided, as defined in CCR Title 15, § 3321;
  - Any documentation of information which contains information or data within any Gang Data Base as defined in the Department Operations Manual (DOM) §§ 52070.22 through 52070.24;
  - Records of investigations, intelligence information, or security procedures as specified in the PRA Section 6254(f).

- Personnel, medical, or similar files, the disclosure of which would constitute an unwarranted invasion of personal privacy protected under the California Government Code § 6254(c) or the Peace Officers Bill of Rights under Government Code §§ 3300 et seq.
- Sensitive Information – information maintained by CDCR that requires a higher than normal assurance of accuracy and completeness. Thus the key factor for sensitive information is that of integrity. Typically, sensitive information includes records of financial transactions and regulatory actions.

Personal Information requested by researchers not under the authority of CDCR may only be received by University of California or other non-profit educational institutions and in accordance with the provisions set forth in law, including the prior review and approval by the Committee for the Protection of Human Subjects (CPHS) of the California Health and Human Services Agency before such information is released (SAM § 5320.5). See Civil Code § 1798.24(t).

### 49020.7 Human Resources Security

CDCR requires that personnel practices related to security management must include:

- Employment history and background checks on all employees.
- The signing of the Computing Technology User Agreement Form 1857 for all staff that uses CDCR's Information Technology, thereby agreeing to abide by CDCR's Workgroup Computing policies.
- The signing of the CDCR Security Awareness Self-Certification and Confidentiality Form ISO-3025 on an annual basis, thereby certifying the employee shall comply with CDCR's Information Security Policy.

### 49020.7.1 Segregation of Duties in the Information Security Program

There shall be a strict separation of duties among, and within, all organizations responsible for using, operating, and developing computer based information systems. Separation of duties shall be maintained to ensure a separation of responsibilities for initiating and authorizing transactions, recording of transactions, and custody of assets. Segregation of duties, similar to that required in manual systems, shall be implemented in computerized systems.

The following guidelines shall be used regarding such separation of duties:

- Convert and Conceal - No one person should be able to convert a resource to their personal use and be able to conceal the action.
- Custody and Control - No one person should have custody of an asset and at the same time be solely responsible for the accounting for that asset.
- Custody and Access - No one person shall have custody of an asset and, at the same time, have unrestricted access to the records pertaining to that asset.
- Origination and Authorization - No one person shall both originate and authorize a transaction.
- Originate and Maintain - No one person shall both enter a transaction and maintain the related master file.
- Access and Restriction - Access to transactions shall be on a need-to-know basis.

EIS is charged with the responsibility for the development and maintenance of computer based systems for the CDCR. In this capacity, EIS provides a service to actual or potential users of computer-based information systems. In addition, there are several computer "user" groups throughout the Department. Each of these organizations is providing a service to all actual or potential users of computer based information systems.

To ensure that assigned responsibilities are met and that separation of duties is maintained, individuals/programs shall not originate or authorize transactions, have custody or control over online data processing assets, or have the authority to originate master file changes. Source documents shall originate and be controlled by functions independent of such persons/programs.

Appropriate procedures shall be developed, subject to approval by the AISO, to ensure that adequate controls exist to ensure the separation of duties and responsibilities.

The procedures may include variances to the Change Management Process in order to resolve failures of critical applications. Such variances shall provide for audit trails and retroactive release or approval documentation, and require the prior approval of the AISO.

### 49020.7.2 Annual Information Security Self Certification

All CDCR employees requiring access to CDCR information assets are responsible for annually self-certifying that they are in compliance with applicable CDCR information security policies. The ISO is responsible for ensuring compliance with this policy. Responsibility for the dissemination of the policies rests with the owner and the designated *ISC*; responsibility for compliance rests with the end-users.

The following is required to ensure compliance with the above is maintained:

- A separate statement of self-certification shall be signed by every employee that accesses or uses CDCR's information assets.
- Each self-certification shall be signed by a representative of the senior management from the organizational entity.
- Each self-certification is to be filed with the local ISC and available for review by the Information Security Office.

### 49020.7.3 Information Security Awareness

It is the responsibility of CDCR management at all levels to ensure that personnel are aware of their responsibilities:

- All employees are accountable for the implementation of information security policies and procedures within their areas of responsibility.
- Accountability requires that employees be aware of the Department's information security policies and procedures.
- All employees that are owners, users, or custodians of a departmental information system shall receive annual information security training.
- Security awareness training shall be given as a part of each employee's orientation and annually thereafter. Each employee shall receive a copy of the security policy. All employees that access or use information assets shall annually complete and sign a self-certification form.
- All employees changing jobs or exiting owner, user, or custodian status, shall have their security privileges reviewed immediately, and such persons shall be prevented from having any further opportunity to access information which they no longer have a business need based on their new job duties.
- Employees with the status of owner, user, or custodian shall have a job description that details that status and the security requirements therein.
- Systems, including CDCR's mission critical systems and Internet access, shall be monitored and activity logs maintained as per the Department's ISSG.

#### 49020.7.3.1 Security Awareness Training within CDCR

All persons who have access to any CDCR information shall be provided security awareness training at the time such access begins and at minimum annually thereafter. The Information Security Coordinators shall ensure that security awareness training is provided prior to the employees' self-certification of their awareness of CDCR's information security policies, and the renewal of access privileges to CDCR information resources.

Security awareness training falls into the following two categories:

- Information Security

- All individuals having access to CDCR information shall be made aware of the background, scope, and objectives of CDCR's information security program and of specific CDCR information security policies and procedures that are applicable to the level and type of access granted to the individual. The minimum training shall consist of completion of the departmental computer-based training module.

- Incident Reporting
  - All CDCR employees shall also be made aware of the events and activities that constitute threats to the organization for which they work and of the actions to be taken when confronted by those events or activities (see DOM § 49020.12).

### 49020.7.4 Consequences of Information Security Violations

During the time that a suspected violation is under investigation, the suspected violator's access privileges may be revoked or other appropriate action taken to prevent harm to the CDCR.

All violations of security policies or procedures are subject to disciplinary action up to and including dismissal from State service. The specific disciplinary action that shall be taken depends upon the nature of the violation and the impact of the violation on the CDCR's information assets and related facilities. For further information see DOM Chapter 3, Article 22, Employee Discipline.

### 49020.7.5 Return of Information Assets

All employees, contractors, and third party users shall immediately return all of the CDCR's information and assets in their possession upon termination of their employment, contract, or agreement.

### 49020.7.6 Removal of Access Rights

Upon termination, position change or change of duties, the access rights of an individual to assets associated with information systems and services shall be evaluated. This will determine whether it is necessary to remove access rights. Changes of employment should be reflected in removal of all access rights that were not approved for the new position. The access rights that should be removed or adapted include physical and logical access, keys, identification cards, information processing facilities, subscriptions, and removal from any documentation that identifies them as a current member of the group. If a departing employee, contractor or third-party user has known passwords for accounts remaining active, these should be changed upon termination or change of employment, contract or agreement.

## 49020.8 Physical Access Control and Environmental Safety

The sensitivity of CDCR's information assets and personnel safety requires that all CDCR computer facilities have physical controls to prevent unauthorized access.

All information resource facilities must be physically protected in proportion to the criticality or importance of their function. Physical access procedures must be documented, and access to such facilities must be controlled. Access lists must be reviewed at least quarterly or more frequently depending on the nature of the systems that are being protected.

Each owner and custodian of departmental information systems shall establish physical controls over their information assets. This requirement applies to workstations with confidential or sensitive information and includes network and data communications components, as well as, application and database servers.

### 49020.8.1 Use of Secure Areas to Protect Data and Information

- Use physical methods to control access to areas. These methods include, but are not limited to, locked doors, secured cage areas, vaults, ID cards, and biometrics.
- Restrict building access to authorized personnel.
- Identify areas within a building that should receive special protection and be designated as a secure area. An example is a server room.

- Security methods should be commensurate with security risk.
- Ensure that physical barriers are used to prevent contamination from external environmental sources.
- Compliance with fire codes.
- Installation, use and maintenance of air handling, cooling, UPS and generator backup to protect the IT investment in server rooms.

### 49020.8.2 Physical Access Management to Protect Data and Information

- Access to facilities that host critical CDCR IT infrastructure, systems and programs must follow the principle of least privileged access. Personnel, including full and part-time staff, contractors and vendors' staff should be granted access to only those facilities and systems that are necessary for the fulfillment of their job responsibilities.
- The process of granting physical access to information resource facilities must include the approval of the Director of EIS, or his/her designee. Access reviews must be conducted at least quarterly, or more frequently, depending on the nature of the systems that are being protected. Removal of individuals who no longer require access must then be completed in a timely manner.
- Access cards and keys must be appropriately protected, not shared or transferred, and returned when no longer needed. Lost or stolen cards/keys must be reported immediately.
- Security clearance for visitors should include, but is not limited to, a sign-in book which includes the date and time of entry and departure, employee escort within a secured area, ID check and ID badges where critical information resources are contained.

### 49020.8.3 Protecting Against External and Environmental Threats

- Consideration shall be given to any security threats presented by neighboring premises, e.g. a fire in a neighboring building, water leaking from the roof or in floors below ground level or an explosion in the street.
- The following guidelines should be considered to avoid damage from the fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster:
  - Hazardous or combustible materials should be stored at a safe distance from a secure area. Bulk supplies such as stationary should not be store within a secure area;
  - Fallback equipment and back-up media should be sited at a safe distance to avoid damage from a disaster affecting the main site;
  - Appropriate firefighting equipment should be provided and suitably placed.

### Working in Secure Areas

Physical protection and guidelines for working in secured areas shall be applied. The following guidelines should be considered:

- Personnel should only be aware of the existence of, or activities within, a secure area on a need to know basis;
- Unsupervised personnel working in secure areas should be avoided both for safety reasons and to prevent opportunities for malicious activities;
- Vacant secure areas should be physically locked and periodically checked;
- Photographic, video, audio or other recording equipment, such as cameras in mobile devices, should not be allowed, unless authorized.

### 49020.8.4 Data Processing Equipment Siting and Protection

Data processing equipment shall be sited and protected to reduce the risks from environment threats and hazards, and opportunities for unauthorized access.

The following guidelines shall be applied to protect equipment:

- Equipment should be sited to minimize unnecessary access into work areas;

- Facilities handling sensitive data should be positioned and the viewing angle restricted to reduce the risk of information be viewed by unauthorized persons during their use, and storage facilities secured to avoid unauthorized access;
- Items requiring special protection should be isolated to reduce the general level of protection required;
- Controls shall be adopted to minimize the risk of potential physical threats, e.g. theft, fire, explosive, smoke, water (or water supply failure), dust, vibration, chemical effects, electrical supply interference, communications interference, electromagnetic radiation, and vandalism;
- Guidelines for eating, drinking, and smoking in proximity to facilities should be established;
- Equipment processing confidential and/or sensitive information shall be protected to minimize the risk of information leakage due to emanation.

### 49020.8.5 Cabling Security

Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage. The following guidelines should be considered:

- Power and telecommunication lines into facilities shall be underground, where possible, or subject to adequate alternative protection;
- Network cabling shall be protected from unauthorized interception or damage, for example by using conduit or by avoiding routes through public areas;
- Power cables should be segregated from communications cables to prevent interference;
- Clearly identifiable cable and equipment markings shall be used to minimize handling errors, such as accidental patching of wrong network cables;
- For sensitive or critical systems further controls to consider include:
  - Installation of armored conduit and locked rooms or boxes at inspection and termination points;
  - Use of alternative routings and/or transmission media providing appropriate security;
  - Use of fiber optic cabling;
  - Use of electromagnetic shielding to protect the cables
  - Initiation of technical sweeps and physical inspections for unauthorized devices being attached to cables;
  - Controlled access to patch panels and cable rooms.

### 49020.8.6 Secure Disposal or Re-Use of Equipment

All items of equipment containing storage media shall be checked by the appropriate IT support staff to ensure that any confidential or sensitive data and licensed software has been removed or securely overwritten prior to disposal.

### 49020.8.7 Removal of Property

Equipment, information or software shall not be taken off-site without prior authorization.

For administrative purposes, all information residing on CDCR's computers that is considered to be sensitive or confidential shall be treated as such by all persons who have access to it and shall be protected from unauthorized access.

### 49020.9 Information Integrity and Data Security

Security controls shall be established to ensure that data entered into and stored in its automated files or databases are complete and accurate, as well as ensuring the accuracy of disseminated information. Security measures will be established to ensure that access is limited to authorized users.

### 49020.9.1 High Risk Confidential Information

No High Risk Confidential Information (HRCI) shall be present on any computer resource, including workstations that are not under the CDCR's direct control unless authorized on a case-by-case basis by the

AISO and the owner of the information unless encrypted using a CDCR approved encryption standard. HRCI is defined as non-public information that if disclosed could result in a significant harm (including financial, legal, risk to life and safety or reputational damage) to the CDCR or individual(s) if compromised through alternation, corruption, loss, misuse, or unauthorized disclosure. Examples of HRCI include, but are not limited to, information such as the following:

- Personally identifiable information such as person's name in conjunction with the person's social security, credit or debit card information, individual financial account, driver's license number, state ID number, or passport number, or a name in conjunction with biometric information;
- Personal health information such as any information about health status, provisions of health care, or payment for health care information as protected under the Health Insurance Portability and Accountability Act of 1996;
- Correctional Offender Record Information as defined in California PC §§ 13100-13104;
- All IT infrastructure information that would reveal vulnerabilities to, or otherwise increase the potential for an attack on, an information technology system of a public agency, including but not limited to firewall and router configurations, server names, IP addresses, and other system configurations;
- Any Document which contains information identifying any Confidential Informant, or information provided, as defined in CCR Title 15, Section 3321;
- Any documentation of information which contains information or data within any Gang Data Base as defined in the DOM §§ 52070.22 through 52070.24;
- Records of investigations, intelligence information, or security procedures as specified in the PRA § 6254(f).

Appropriate procedures to utilize confidential CDCR information on any of CDCR's computer resources, including any computer such as mainframes, servers, workstation, and other information assets on the CDCR network are outlined in this Article. The level of security measures shall be commensurate with the data classification of the information involved.

### 49020.9.2 Confidentiality of Security Mechanisms

The specific security mechanisms used by the Department to control access to its information resources are confidential.

Information concerning specific details of access controls shall not be divulged except on a need-to-know basis, and then only to persons for whom there are signed security agreements on file.

### 49020.9.3 Confidentiality of Production Application Software

All documentation concerning production applications residing on the CDCR's mainframes, servers, network infrastructure, and workstations is confidential.

Appropriate procedures to protect and preserve the confidentiality of an application's documentation are to be developed by the data custodian that has responsibility for, or custody of, such application. The procedures shall ensure that documentation is not divulged except on a need-to-know basis, and then only to persons for whom there are signed security agreements on file.

### 49020.9.4 Confidentiality of Information on CDCR Information Systems

Appropriate procedures shall be developed by the appropriate data custodians to protect and preserve the confidentiality of the Department's information stored or residing in or on CDCR controlled environments, such as the CDCR Network, individual stand-alone desktop and laptop workstations, browser-based applications such as Parole-LEADS, and the SOMS. Additionally, no High Risk Confidential Information shall be faxed, reproduced (e.g., photocopied), distributed via unencrypted e-mail, downloaded to a non-confidential system, given to an unauthorized recipient, or transmitted by telephone to any entity without appropriate security controls in place that are documented in the CDCR ISSG.

### 49020.9.5 Confidentiality Agreements

Requirements for confidentiality or non-disclosure agreements reflecting the CDCR's needs for the protection of information should be identified and regularly reviewed. Confidentiality and non-disclosure agreements protect organizational information and inform signatories of their responsibility to protect, use, and disclose information in a responsible and authorized manner.

Confidentiality or non-disclosure agreements should address the requirement to protect confidential information using legally enforceable terms. To identify requirements for confidentiality or non-disclosure agreements, the following elements should be considered:

- A definition of the information to be protected (e.g., confidential information);
- Expected duration of an agreement, including cases where confidentiality might need to be maintained indefinitely;
- Required actions when an agreement is terminated;
- Responsibilities and actions of signatories to avoid unauthorized information disclosure (such as "need to know");
- Ownership of information, trade secrets and intellectual property, and how this relates to the protection of confidential information;
- The permitted use of confidential information, and rights of the signatory to use information;
- The right to audit and monitor activities that involve confidential information;
- Process for notification and reporting of unauthorized disclosure or confidential information breaches;
- Terms for information to be returned or destroyed at agreement cessation; and
- Expected actions to be taken in case of a breach of this agreement.

Based on the CDCR's security requirements, other elements may be needed in a confidentiality or non-disclosure agreement. Confidentiality and non-disclosure agreements should comply with all applicable laws and regulations for the jurisdiction to which it applies. Requirements for confidentiality and non-disclosure agreements should be previewed periodically and when changes occur that influence these requirements.

### 49020.9.6 Information Sharing with External Parties

The risk to CDCR's information and facilities from business processes involving external parties should be identified and appropriate controls implemented before granting access.

When there is a need to allow an external party access to the facilities or information of the CDCR, a risk assessment should be carried out to identify any requirements for specific controls. The identification of risks related to external party access should take into account the following issues:

- The facilities an external party is required to access;
- The type of access the external party will have to the information and facilities, e.g., physical access to offices, computer rooms, filing cabinets or logical access to an organization's databases and information systems;
- Network connectivity between the organization's and the external party's network(s), e.g., permanent connection, remote access;
- Whether the access is taking place on-site or off-site;
- The value and sensitivity of the information involved, and its criticality for business operations;
- The controls necessary to protect information that is not intended to be accessible by external parties;
- The external party personnel involved in handling the organization's information;
- How the organization or personnel authorized to have access can be identified, the authorization verified, and how often this needs to be reconfirmed;
- The controls employed by the external party when storing, processing, communicating, sharing, and exchanging information;

- The impact of access not being available to the external party when required, and the external party's entering or receiving inaccurate or misleading information;
- Practices and procedures to deal with information security incidents and potential damages, and the terms and conditions for the continuation of external party access in the case of an information security incident;
- Legal and regulatory requirements and other contractual obligations relevant to the external party that should be taken into account; and
- How the interests of any other stakeholders may be affected by the arrangements. Access by external parties to the CDCR's information should not be provided until the appropriate controls have been implemented and, where feasible, a Data Sharing Agreement (DSA) or Memorandum of Understanding (MOU) has been signed, defining the terms and conditions for the connection or access and the working arrangement. Generally, all security requirements resulting from work with external parties or internal controls should be reflected by the agreement with the external party.

It should be ensured that the external party is aware of their obligations, and accepts the responsibilities and liabilities involved in accessing, processing, communicating, or managing the organization's information and facilities.

### 49020.9.7 Personal Computer Security

Information maintained in a personal computer system, including laptop computers and mobile devices, must be subjected to the same degree of management control and verification of accuracy that is provided for information that is maintained in other automated files. Files containing High Risk Confidential Information or sensitive data shall not be stored in personal computer systems unless it can be demonstrated that doing so is in the best interest of CDCR and that security measures have been implemented to provide adequate protection. Proposals to use desktop or laptop computers to maintain or access files containing High Risk Confidential Information or sensitive data must be approved by the Agency Information Security Officer (SAM § 5315.1) before implementation. The Agency Information Security Officer will determine that the proposal complies with all applicable provisions of the SAM dealing with information security and risk management (SAM §§ 5300 through 5399).

### 49020.9.8 Personal Computing Devices

Using personally-owned devices to access departmental information resources may jeopardize the integrity and security of CDCR's information resources. In regard to personally-owned devices, the following provisions shall be followed:

- Personally-owned electronic devices shall not connect to, transfer data to or from, or be used to copy data to or from the CDCR Network;
- Personally-owned smartphones such as Android devices, iPhones, Treos, Blackberry devices shall not connect to, transfer data to or from, or be used to copy data to or from the CDCR Network. CDCR e-mail shall not be setup for delivery or used on any personally-owned Smartphone or electronic device;
- Personally-owned USB memory "sticks," "cards," or "external drives" shall not be used to copy, forward, or transfer CDCR data from CDCR local drives, networks, or e-mail systems.

Exemptions to these provisions shall require approval from all impacted data owners and the Agency Information Security Officer.

### 49020.9.9 Mobile Computing and Storage Devices

All mobile computing and storage devices that access the CDCR network and/or store CDCR data must be compliant with CDCR Information Security Policies and Standards. In regard to mobile computing and storage devices, the following provisions shall be followed:

- High Risk Confidential Information on any stored on mobile computing and storage devices must be encrypted;

- Any and all mobile computing devices used within the CDCR information and computing environments must meet all applicable CDCR encryption standards. Mobile computing devices shall be tracked in an information assets inventory;
- CDCR information security policies applicable to desktop or workstation computers apply to mobile computing devices;
- Employees will delete information from their portable device or portable storage media once it is no longer needed;
- All CDCR laptops shall connect to the CDCR network at a minimum of 42 days or another designated time frame to receive updates;
- Personal long distance calls shall not be made from state-issued handheld devices except as authorized in DOM Chapter 1 Organizational Structure, Article 12 – Telephones, Facsimiles, and Cellular Type Telephones.
- Personal local calls shall not be made from state-issued handheld devices except as authorized in DOM Chapter 1 Organizational Structure, Article 12 – Telephones, Facsimiles, and Cellular Type Telephones.

### 49020.10 Access Control

Access to any of the CDCR's computerized information on any of the CDCR's computers or the OTech Data Center is restricted to authorized persons. All access to CDCR's information systems shall be protected by at least user ID/password access control. Any software installed on information systems which use password protection features shall provide for non-display of, and restricted control over, passwords. No software that allows the authentication process to be bypassed or comprised may be installed on those computers.

- Any person requiring such access shall:
- Be a State employee or a bona fide representative of the Department.
- Demonstrate either a need for, or a legal right to, the information.
- Receive formal authorization from the owner of the information.
- Accept legal responsibility for preserving the security of the information.

The sensitivity of the information residing in the CDCR's computerized environments requires strict controls over who is allowed access to that environment, which information may be accessed, and how that information may be accessed.

The following uniform access authorization procedure assumes that all pertinent procedures have been followed, and all CDCR-required system approvals have been obtained. This policy is for access to existing information resources. The uniform access authorization procedure is as follows.

- All access requests shall be sent to the system owner with a copy to the AISO. The request shall contain the following:
  - The name of the requester.
  - The specific information for which access is desired.
  - The reason(s) why the requestor has a need for, or right to, the information.
  - The frequency and duration of the requested access.
  - The type of access (e.g., read, update, copy, etc.).

After the data owner approves the request for access and returns it to the requestor, the approval is then routed to either EIS or the requesting organization's ISC for action.

### 49020.10.1 Information Security-Responsibilities of Password Owners

Access to CDCR's information systems is restricted by password to only authorized persons. Authorized persons shall never reveal their passwords to anyone for any reason. Authorized persons using a computer shall log off or activate a password-protected screensaver before leaving the immediate vicinity of the computer or terminal. Additionally, no ability shall exist for a user to store, load, or invoke the log on

process on any CDCR computer, by any method that includes the user Resource Access Control Facility (RACF), ID, or the password. Violation of this Policy may result in the revocation of all access privileges and appropriate disciplinary action. Such disciplinary action may be based not only on the violation itself, but also on all activity performed by those obtaining access to a system or information asset due to a violation of this Policy.

The password is a major "key" to the integrity of CDCR's automated environment. The password policy exists to protect the integrity of that "key."

User IDs shall never be duplicated. User ID security is backed up by the existence of passwords. Owners are responsible for anything for which their password is used. Therefore, as a matter of self-protection, the password owner shall:

- Not tell anyone what their password is.
- Not write down their password.
- Not use an obvious password. Obvious passwords include one's name or nickname, the names of one's children, one's user ID, names, or words associated with hobbies ("DANCER," "SKIER," "GOLFER," etc.), names associated with favorite books, TV shows, or movies ("JEDI," "FRODO," "PICARD", "RHETT," etc.), "SECRET," "SECURE," "PASSWORD," all spaces or the "enter" key, "9999999", "XXXXXXX," driver's license, social security numbers, the name of the current month, etc.
- Not use words that can be looked up in any dictionary, including foreign languages (e.g., Latin).
- Use non-obvious passwords, such as word combinations rather than single words ("COMPUTERUSER," "SKIBUM," "IAMADANCER," etc.) intentionally misspelled words ("KRAKER," "KORECTUNS," etc.), or random combinations of letters and numbers, etc.
- Use passwords that are at least eight characters long.
- Change the password in accordance with specific application requirements, every 30 to 90 days, depending on the application.

If the password owner becomes aware that a correct password is being rejected, that user should immediately notify the local ISC and the AISO, since this may indicate that someone has discovered the password and has changed it without the owner's permission, resulting in the owner no longer knowing his or her own password.

If a password is forgotten, the local IT support staff or the CDCR Help Desk shall be contacted for a password reset. They shall validate the owner's identity and give a new temporary, one-time password. The owner shall change this password immediately.

If anyone asks for a password, the owner shall refuse to provide it and shall refer the person to a supervisor. The owner shall then notify the supervisor.

Anyone who knows that any password has been compromised should take the following actions:

- Notify the ISC;
- Notify the immediate manager/supervisor;
- Notify the Information Security Office;
- Complete a "security incident report " and submit it to the Information Security Office.

### 49020.10.2 Information Security-Responsibilities of Supervisors

People are provided passwords because their jobs require them to access CDCR information systems. When a password owner terminates employment or is reassigned to duties that do not require such access, the immediate supervisor shall, without delay, notify the applicable party of the change.

The authority to access CDCR computers entails a significant risk to the Department's ability to function. Such authority is restricted to persons with a demonstrated need for access. Because that need is, by definition, a function of the person's specific job duties, any change in those duties requires a reevaluation of the need for access. If the duties change such that the need for access no longer exists, the access shall be revoked.

If any password owner changes job duties (via resignation, promotion, transfer, reorganization, separation, etc.), that individual's immediate supervisor shall initiate the following:

- Reevaluate whether the person's new duties still require the authority to access CDCR's computers.
- Notify the local IT support staff or the access management group if the person no longer requires access authority.
- Notify the owner of the relevant CDCR information so that the appropriate paperwork can be initiated to document the removal of the person's access privileges if the person no longer requires access authority.

The lack of use of the access authority is assumed to be proof that the authority is no longer required. Access authority to information assets may be revoked without notice if they are not used regularly.

### 49020.10.3 Requesting Authority to Access CDCR's Mainframe Environments

Access to an entire mainframe environment shall not be authorized. Access to specific portions of that environment, such as, but not limited to, the system development facilities, shall be authorized for specific organizations. Access to a specific application can be authorized by the Information Owner as a means of meeting a specific request for specific information.

### 49020.10.4 Unattended Workstations

Active workstations or terminal sessions must not be left unattended. Any authorized or unauthorized activity on an unattended workstation will be attributed to the person whose logon and password activated the terminal or workstation. All sessions shall either be terminated when leaving the immediate area, or protected with a password-activated screensaver.

### 49020.10.5 Restrictions on Using CDCR Information Assets

The use of all CDCR information assets including any mainframe computers, servers, notebook, laptop and workstation desktop systems, network components, and applications run on or accessed from CDCR computers is restricted to official CDCR business.

### 49020.10.6 Reassignment of Workstations

The local computer coordinators shall erase all electronic documents from the hard drive of a computer once any staff member of the CDCR has ceased using that computer. All forms of electronic documents that the previous staff member created, received, or used shall be removed. As needed, the electronic documents may be transferred to another computer. Notification of the previous staff member’s being placed on litigation hold or being under investigation requires that the information be stored and properly secured until further notification.

## 49020.11 Information Systems Acquisitions, Development and Maintenance

Information systems include operating systems, infrastructure, business applications, off-the-shelf products, services, and user-developed applications. The design and implementation of the information system supporting the business process can be crucial to security. Security requirements shall be identified and agreed upon prior to the development and/or implementation of information systems. All security requirements shall be identified at the requirements phase of a project and justified, agreed upon, and documented as part of the overall business case for an information system.

### 49020.11.1 Correct Processing in Applications

Appropriate controls shall be designed into applications to ensure correct processing. These controls should include data validation of input data, internal processing and output data. Additional controls may be required for systems that process, or have an impact on, sensitive, valuable or critical information.

### 49020.11.1.1 Input Data Validation

Checks shall be applied to the input of transactions. The following guidelines should be considered:

- Dual input or other input checks, such as boundary checking or limiting fields to specific ranges of input data;
- Periodic review of the content of key fields or data files to confirm their validity and integrity;
- Inspecting hard-copy input documents for any unauthorized changes (all changes to input documents should be authorized);
- Procedures for responding to validation errors;
- Procedures for testing the plausibility of the input data;
- Defining the responsibilities of all personnel involved in the data input process;
- Creating a log of the activities involved in the data input process.

### 49020.11.1.2 Message Integrity

An assessment of security risks should be carried out to determine whether message integrity is required and to identify the most appropriate method of implementation. Data output from an application shall be validated to ensure that the processing of stored information is correct.

Output validation may include:

- Plausibility checks to test whether the output data is reasonable;
- Reconciliation control counts to ensure processing of all data;
- Providing sufficient information for a reader or subsequent processing system to determine the accuracy, completeness, precision, and classification of the information;
- Procedures for responding to output validation tests;
- Defining the responsibilities of all personnel involved in the data output process;
- Creating a log of activities in the data output validation process.

### 49020.11.2 Cryptographic Controls

Cryptographic controls should be considered to achieve:

- Confidentiality: using encryption of information to protect sensitive or critical information either stored or transmitted;
- Integrity/authenticity: using digital signatures or message authentication codes to protect the authenticity and integrity of stored or transmitted sensitive or critical information;
- Non-repudiation: using cryptographic techniques to obtain proof of the occurrence or non-occurrence of an event or action.

Based on a risk assessment, the required level of protection shall be identified taking into account the type, strength, and quality of the encryption algorithm required. All cryptographic keys shall be protected against modification, loss, and/or destruction.

### 49020.11.3 Security of System Files

To minimize the risk of corruption to operation systems, the following procedures shall be implemented:

- The updating of operation software, applications, and program libraries, shall only be performed by trained administrators upon management authorization;
- Operational systems shall only contain approved executable code, and not development code or compilers;
- A rollback strategy shall be in place before changes are implemented;
- An audit log shall be maintained of all updates to operational program libraries;
- Previous versions of application software shall be retained as a contingency measure.

Decisions to upgrade to a new software release should take into account the business requirements for the change, and the security of the release, i.e. the introduction of new security functionality or the number and

severity of security problems affecting this version. Software patches shall be applied when they can help to remove or reduce security weaknesses.

Physical or logical access shall only be given to non-CDCR employees for support services when necessary, and with approval from the AISO. Access to CDCR information resources should be monitored. Computer software that relies on externally supplied software and modules shall be monitored and controlled to avoid unauthorized changes, which could introduce security weaknesses.

### 49020.11.4 Protection of System Data

The use of operational databases containing personal information or any other sensitive information for testing purposes should be avoided. If personal or otherwise sensitive information is used for testing purposes, all sensitive details and content should be removed or modified beyond recognition before use.

### 49020.11.5 Access Control to Program Source Code

Access to program source code and associated items (such as designs, specifications, verification plans and validation plans) shall be strictly controlled, in order to prevent the introduction of unauthorized functionality and to avoid unintentional changes.

### 49020.11.6 Security in Development and Support Processes

Ensuring the security of application system software and information is essential. As such, production environments shall be strictly controlled.

### 49020.11.6.1 Change Control Procedures

Formal change control procedures shall be documented and enforced in order to minimize the corruption of information systems. Introduction of new systems and all changes that could possibly have an impact on the users or system availability shall follow a formal process of documentation, specification, testing, quality control, and managed implementation.

This process shall include an analysis of the impacts of changes, and specification of security controls needed. This process shall also ensure that existing security and control procedures are not compromised, that support programmers are given access only to those parts of the system necessary to perform or complete their work, and that formal agreement and approval for any change is obtained.

The following operational change control procedures shall be integrated:

- Maintain a record of the agreed authorization levels;
- Ensure changes are submitted by authorization users and have management approval;
- Review controls and integrity procedures to ensure that nothing will not be compromised by the changes;
- Identify all software, information, database entities, and hardware that require amendment;
- Obtain form approval from the Change Control Board before work commences;
- Ensure system documentation is updated on the completion of the change and that old documentation is archived or disposed of;
- Maintain version control for all software updates;
- Maintain an audit trail of change requests;
- Ensure that operating documentation and user procedures are changed as necessary to remain appropriate;
- Ensure that the implementation of changes take place at the right time and does not have a significant impact to the business involved.

### 49020.11.6.2 Technical Review of Applications after Operating System Changes

When operating systems are changed, critical business applications shall be reviewed and tested to ensure there is no adverse impact on operations or security.

### 49020.11.6.3 Outsourced Software Development

Outsourced software development shall be supervised and monitored by EIS.

## 49020.12 Incident Management

To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective actions to be taken, formal event reporting and escalation procedures shall be in place. All employees, contractors and third-party users shall be made aware of the procedures for reporting the different types of events and weaknesses that might have an impact on the security of the CDCR's information assets.

**Incident Reporting**

It is the responsibility of all departmental employees to report all incidents that would place the Department's information assets at risk. The following incidents shall be reported through the local ISC to the Information Security Office within three days of becoming aware that a security incident has occurred:

- Unauthorized access to, or modification of, State-owned or State-managed data, including non-electronic data such as reports, documentation, and hard copy files.
- Unauthorized use of, or access to, State computer resources, including computer networks and services as well as systems not necessarily connected to a network.
- Unauthorized access to, or modification of, computer software, including operating systems, networks, configurations, and applications. This includes the introduction of malicious software such as viruses, worms, and other malicious software.
- Deliberate or unauthorized acts resulting in disruption of State computer services, including "Denial of Service" attacks.
- Unauthorized use of user account or Internet domain names.
- Destruction of, or damage to, State facilities and/or information assets.
- Break-in or other unauthorized access to State facilities resulting in compromise to the data or computer systems housed within those facilities.
- Security weaknesses that pose a threat to CDCR information resources.

The Information Security Office shall investigate all incidents.

### 49020.12.1 Incident Report Format

The following information concerning each incident shall be reported to the Information Security Office within three working days of becoming aware of the occurrence of the incident:

- Date and time.
- Location.
- Description of what happened.
- Estimated damages.
- Description of corrective action taken or planned.
- Estimated costs associated with corrective actions.
- If known, identity of those responsible for the incident.
- Descriptions of actions taken or planned against those responsible for the incident.
- Contact name and phone number of the person reporting the incident.

The report submitted to the Information Security Office shall be signed by the appropriate Warden, Regional Parole Administrator, Director, or Assistant Secretary.

Incidents involving the following shall be forwarded to the State Office of Information Services (OIS) within five business days of the initial report, and shall be signed by the AISO and Secretary or there authorized delegate:

- CDCR-owned or CDCR managed data, without authorization, was damaged, destroyed, deleted, shared, altered, or copied, or used for non-state business. This includes computer documentation and configuration information, as well as electronic and non-electronic data and reports.
- Unauthorized parties accessed one or more CDCR computers, computer systems, or computer networks. This includes deliberate and unauthorized uses of CDCR-owned computer services, as well as, "hacker attacks."
- Someone has accessed and without permission added, altered, damaged, deleted, or destroyed any computer programs which reside or exist internal or external to a CDCR computer, computer system, or computer network.
- Disruption of CDCR computer services or denial of computer services occurred in a manner that appears to have been caused by deliberate and unauthorized acts.
- A contaminant was introduced into a CDCR computer, computer system, or computer network. This includes, but is not limited to, viruses, Trojans, worms, and other types of malicious attacks.
- Internet domain names and/or users account names have been used without permission in connection with the sending of one or more electronic mail messages, and thereby caused damage to a CDCR computer, computer system, or computer network, or misrepresented CDCR or CDCR employees in electronic communications.
- Damage or destruction of CDCR information processing facilities has occurred.
- Physical intrusions into CDCR facilities have occurred that may have resulted in the compromise of CDCR data or computer systems.
- Lost, damaged, or stolen devices used for information processing.

The California Highway Patrol's Emergency Notification and Tactical Alert Center (ENTAC) shall be notified of the occurrence of an incident within one day of receipt of the initial report. Incidents involving "Personally Identifiable Information" (PII) or "Personal Health Information" (PHI) involving more than 500 California Residents shall be reported to the Attorney General.

### 49020.12.2 Collection of Evidence

When misconduct is discovered which constitutes an information security incident in conjunction with a possible violation of departmental policy or criminal violation, precaution must be taken to avoid contamination of the possible electronic evidence. Prior to taking action, the discoverer should contact the Hiring Authority and/or the Office of Internal Affairs (OIA) for direction, if the misconduct could lead to an administrative investigation. If the misconduct rises to the level of criminal misconduct, the OIA must be notified immediately prior to any action being taken.

When there is any incident that involves the preservation of any evidence and after the first responder has consulted with the Hiring Authority/OIA, the first responder is responsible to preserve the electronic crime scene and recognize, collect, and safeguard the digital evidence and/or non-digital evidence. First responders and managers who supervise personnel who process such events should be familiar with the information in this section and perform their duties.

Digital evidence includes all information and data of value to an investigation that is stored on, received, or transmitted by an electronic device. All other evidence is non-digital evidence.

When dealing with digital evidence, general forensic and procedural principles should be applied:

- The process of collecting, securing, and transporting digital evidence should never change the evidence and integrity of the chain of evidence must be maintained.
- Digital evidence should only be examined and/or acquired by those trained specifically for that purpose. First responders without proper training, equipment, or skills should not attempt to explore the contents of or to recover information from any electronic device.
- Everything done during the seizure, transportation, and storage of digital evidence should be fully documented, and preserved. Documentation should include the specific location of the evidence found, how it was collected, labeled, and preserved.
- Package and transport digital evidence in a secure manner consistent with chain of evidence procedures.
- Any Forensic work shall be performed on copies of the digital evidence. The original device(s) shall be secured and protected for the entire process until a matter has been determined closed. The original drive shall not be imaged or cloned without consulting first with the OIA.

When dealing with all other forms of non-digital evidence:

- The original evidence shall be kept securely with a record of the individual who located it.
- The individual who located the original evidence shall prepare a record of the location of the evidence, when the evidence was found, who witnessed the discovery of the evidence.
- Package and transport of non-digital evidence in a secure manner consistent with chain of evidence procedures.

### 49020.13 Failure to Correct Information Security Deficiencies

Should any audit indicate that the State's security policies are not established or that the Department has not taken corrective action with respect to security deficiencies, the Department may be subject to any or all of the following:

- Further audit and review by the Department of Finance (DOF), Bureau of State Audits (BSA), State Controller's Office (SCO), and/or Department of Justice (DOJ).
- Revocation by the DOF of delegated approval authority for IT projects.
- Application of penalties specified in GC § 1222.

### 49020.14 Technical Vulnerabilities Management

Technical vulnerability management shall be implemented in an effective, systematic, and repeatable way with measurements taken to confirm its effectiveness.

A current and complete inventory of information assets will be maintained. Specific information gathered should include software vendor, version numbers, software installed and person(s) responsible for the software installation. Appropriate timely action shall be taken in response to the identification of potential technical vulnerabilities. The following should be established:

- EIS shall define and establish the roles and responsibilities associated with technical vulnerability management, including vulnerability monitoring, vulnerability risk assessment, patching, asset tracking, and any coordination responsibilities required;
- Information resources that will be used to identify relevant technical vulnerabilities and to maintain awareness about them should be identified for software and other technology (based on the asset inventory list,); these information resources should be updated based on changes in the inventory, or when other new or useful resources are found;
- A timeline should be defined to react to notifications of potentially relevant technical vulnerabilities;
- Once a potential technical vulnerability has been identified, EIS shall identify the associated risks and the actions to be taken;

- Depending on the urgency of which a technical vulnerability needs to be addressed, the action taken shall be carried out according to change control procedures or by following the Department's information security incident response procedures;
- If a patch is available, the risks associated with installing the patch should be assessed (the risks posed by the vulnerability should be compared with the risk of installing the patch;
- Patches should be tested and evaluated before they are installed to ensure they are effective and do not result in side effects that cannot be tolerated; if no patch is available, other controls should be considered, such as:
  - Turning off services or capabilities related the vulnerability
  - Adapting or adding access controls, e.g. firewall rules, at the network border;
  - Increased monitoring to detect or prevent actual attacks;
  - Raising awareness of the vulnerability.

Employees, contractors, and third-party users of information systems and services shall not attempt to prove suspected security vulnerabilities. Testing vulnerabilities may be interpreted as a potential misuse of the system and could cause damage to the information system or service and result in disciplinary actions for the individual performing the test.

### 49020.15 Confidential or Sensitive Information Stored on Workstations

The nature of information classified as confidential or sensitive requires strict controls over access to such assets (SAM § 5335.2). Files containing confidential or sensitive data (as defined in SAM § 5335.2) should not be stored in personal computer systems unless it has been demonstrated that doing so is in the best interest of the Department and that security measures have been implemented to provide adequate protection and approval from the AISO has been given.

With the aforementioned approval, confidential or sensitive information may be stored on or accessed with workstations in accordance with the following provisions:

- Only authorized personnel may have access to confidential or sensitive data.
- Workstations containing or capable of accessing such data shall be equipped with hardware and/or software that provide for authentication techniques, such as password protection of confidential files.
- HRCI and sensitive files shall be encrypted, if the owner deems it necessary. Encryption software must comply with standards documented in the AISO's ISSG.
- Backup files of confidential data shall be maintained in a locked cabinet away from the location of the workstation containing the program providing access to such files.
- Security hardware/software shall comply with standards documented in the ISSG.
- At least two individuals shall be authorized access and have knowledge of the location where data files, backup files, and forms are stored.

### 49020.15.1 Software Controls on CDCR's Workstations

The following software controls shall be established for all CDCR workstations:

- No software shall be loaded, installed, and/or activated on any CDCR workstation without prior review and written approval from the local ISC and the requestor's supervisor, or EIS.
- Controls that ensure that the CDCR is in compliance with all State-mandated requirements (SAM, §§ 5310, 5345.1).
- Appropriate procedures shall be developed by ISCs for use by each CDCR division that has workstations. These procedures are subject to approval by the AISO, and are constrained by the requirements of the CDCR workstation policy.

### 49020.15.2 Data File Transfers

Electronic transfer (file transfer) of information to or from any CDCR information system file or database is restricted to authorized persons who shall use an approved file transfer mechanism. The same level of

protection afforded the information in its originating system shall be provided by the computer environment to which the information is transferred.

Transfer of information from one CDCR computer to another does not alter the sensitive nature of the information or eliminate the need to protect the confidentiality of the information. An appropriate procedure shall be developed by EIS for use by each CDCR division that uses file transfer mechanisms. The procedure shall be constrained as follows:

- The user is responsible for providing the necessary controls to secure all confidential information maintained in the workstation environment. A Security Plan must be approved by the ISO prior to High Risk Confidential Information or sensitive information being stored on a workstation.
- Dial-up access to the Department's databases is prohibited without explicit authorization from the data owner and Information Security Office.
- All requests to transfer information shall be approved by the owners of the information and the custodians of the information. The owners shall provide the necessary authorization for access (if the request is approved) and the custodian shall provide the methodology.
- Confidentiality and integrity of information shall be maintained.
- Any workstation performing file transfers shall be subject to additional hardware and software controls (e.g., encryption and dynamic password user authentication) to enhance the security environment of the workstation.

### 49020.16 Information Security Standards and Guidelines

Data processing equipment in CDCR's automated network environment (computers and peripherals) shall be secured against access by unauthorized persons. Any equipment that is not stand-alone is considered data processing equipment. This includes all workstations that are connected to each other or to any other server or mainframe, system, whether by dial-up, cabling (including, but not limited to, coax, twisted pair, and fiber), LANs, gateways, routers, and all other network components. Access to CDCR's network shall be restricted to CDCR employees and approved consultants. The methods by which CDCR's data processing equipment is secured shall be documented in the CDCR ISSG. Any exception or modification to the ISSG must be approved in writing by the AISO prior to implementation.

The ISSG shall include descriptions of procedures to protect and preserve the data processing equipment from access by unauthorized persons. The procedures are constrained by the following:

- Only authorized personnel shall have access to terminals, printers, control units, concentrators, telephone wiring panels, modems, and emulation cards.
- Control of access through the CDCR telecommunications system to the Internet is the responsibility of the EIS, and is administered in accordance with the ISSG. Additional access not described in the ISSG constitutes a request for a modification to the ISSG and must be submitted and approved in accordance with this policy prior to implementation.
- Persons not authorized to access the CDCR's telecommunications system shall obtain approval from the designated local ISC. Unauthorized persons include representatives of control agencies, CDCR personnel from another site, equipment vendors, telephone companies, etc.
- Any division with custodianship of decentralized applications shall locate equipment in restricted areas that shall be monitored during working hours and locked during unattended periods.
- Access to computers, either connected to a CDCR network or stand-alone, shall be limited by the use of a password-protected screensaver and/or key-controlled access to the power supply and/or keyboard with the keys physically removed and stored away from the workstation.
- Computers connected in any way to CDCR's telecommunications system or stand-alone computers with modems connected to them may not be located in areas where inmates have access, except for work assignments when the inmates are under the direct and constant supervision of custody staff.
- Control units shall be locked whenever possible and the keys removed and stored in a secure environment.

- Storage media including, but not limited to, diskettes, CDs, removable hard drives, and tapes shall be removed from equipment that reads them and stored in a secure environment when not in use.
- Documentation pertaining to the hardware, system software, and configuration of the CDCR's telecommunication system are confidential.
- All facility phone rooms and other locations where network components are kept shall be labeled "Out of Bounds. Authorized Personnel Only."

### 49020.16.1 Requests for Modifications of the Information Security Architecture ISSG

The sensitivity of the CDCR's automated information assets requires strict controls over who can use equipment that is configured to access these assets. Also, the monetary value of the equipment itself warrants physical controls to deter theft or damage to the equipment. Requests for modification of the ISSG shall be submitted to the AISO.

### 49020.17 Modem Usage

The critical and sensitive nature of the informational resources residing in CDCR's computers requires stringent controls of devices attached to these computers, and over which persons are allowed to use these devices.

All access to the CDCR's systems shall be monitored and controlled by EIS. All other means of accessing CDCR systems including, but not limited to, wireless communication devices and dialup modem, are prohibited unless approved by the ISO.

Modem use is restricted to computers not connected to the CDCR Network, unless such use is an approved part of the ISA. Requests for additional modems to be used within the CDCR teleprocessing environment are subject to approval.

Modems may be used to access remotely the CDCR network resources through EIS-supported access mechanisms. They may also be used to provide access to the Internet and specific destinations and e-mail capability when such access is not available through the CDCR network resources. Justification and procurement of modems for these purposes shall be conducted in accordance with DOM, Chapter 4, Article 41, Departmental Workgroup Computing Policy.

Specific restrictions on the use of modems are:

- There shall be no inmate or parolee access to any computer for which a modem has been approved. Computers that are attached to modems shall not be located in areas where inmates or parolees have access.
- No applications that were developed by inmates shall be implemented on a modem-equipped computer.
- No modems shall be installed on any computer that is a part of a LAN that has been approved for inmate use.
- The location and usage of all modems must be tracked and monitored at all times.
- Computers with "pocket" modems may not be used within the secured perimeter of facilities. They shall not be used in parole offices unless the area where the modem is to be used is secured from parolee access.
- Non-CDCR computers shall not access the CDCR Network via modem.

### 49020.18 Inmate/Ward Use of Computers

It is the policy of the Department to allow inmates, wards or parolees access to computers, computer terminals, or computer keyboards only within the constraints of the policies contained in this Article. For the purpose of this section, "Inmate" means a male or female offender who is committed under sentence to or confined in a penal or correctional institution under the authority of CDCR, which includes youth offenders under the jurisdiction of the CDCR's Division of Juvenile Justice. Any request for exception shall be referred to the AISO for review.

### 49020.18.1 Restrictions on Computer-Knowledgeable Inmates

Inmates who have a history of computer fraud or abuse, as defined in Penal Code (PC), § 502, shall not be placed in any assignment that provides access to a computer.

Inmates that have documented histories of computer fraud or abuse, as noted during the initial classification process, shall be identified on the initial classification chrono. Any occurrence of computer abuse after admittance to the prison system shall also be recorded in the inmate's records.

Inmates who have knowledge of computer use, programming experience, or other skills that exceed assigned staffs' ability to monitor their activity on computers, may be restricted from having access to computers. Staff assigned to supervise inmates using computers must be able to monitor inmates' activity.

### 49020.18.2 Inmate Access to Computer-Based Tools

Inmates shall not be allowed access to any computer-based tools that could be utilized to create a virus, Trojan Horse, worm, or cause damage to data files or a computer's operating system, except in an approved Computer Refurbishment Program.

### 49020.18.3 Inmate Access to Computers and Telecommunications Devices

Inmates may access workstations for the purpose of completing specific tasks or assignments while under direct and constant supervision. The approved uses of workstations by inmates shall be carried out only under very tightly controlled circumstances:

- Each computer shall be labeled to indicate whether inmate access is authorized.
- Computers used by inmates shall not be used concurrently for any other purpose.
- The local ISC shall approve or disapprove the movement of computers from an "inmate use" status to other work and vice versa.
- Any computer that is being repurposed from employee use to inmate use shall have the hard drive erased of all data prior to the redeployment using the methods in the department's data wiping standards.
- Inmates with a work assignment involving a particular computer shall not be assigned to work on other computers.
- Areas where inmates are authorized to work on computers shall be posted as such.
- All inmates shall be under the supervision of a knowledgeable employee within a controlled, designated area when using computers.
- There shall be no communications capabilities in the designated area, such as a telephone line, computer network line, telephone punch panel, cell phones, wireless communication devices such as pagers or handheld computers or radio communication devices without approval of the AISO.
- Inmates shall not have access to computer utility programs used to modify the functionality of the computer or to view system configuration information, except in an approved Computer Refurbishment Program.
- Inmates shall not have electronic storage media in their possession except within an approved area.
- Inmates may not have access to computer application development tools.
- An inventory and appropriate controls shall be maintained on all portable storage media. Portable storage media for inmate use shall be labeled "For Inmate Use." Reports and other printed output from inmate-utilized computers shall be reviewed closely by staff, and appropriate distribution of such output shall be monitored.
- Inmates shall not have access to the operating system of any computer. Inmates shall not have access to any interface that allows access to the system configuration of any computer including, but not limited to, dialogue boxes, setup, and configuration screens. Additionally, inmates shall not have access to operating system commands that allow viewing or modification of any aspect of a computer operating system or the configuration of a computer, except in an approved Computer Refurbishment Program.
- Inmates shall not be allowed to load software onto hard disks, except in an approved Computer Refurbishment Program.

- No inmate shall have access to, or possession of, any telecommunication capability, including Internet accessible computers, wireless devices such as pagers or handheld computing devices or cell phones without approval from the Agency Information Security Officer.
- There shall be no inmate access to a computer outside the inmate's authorized work, vocational, or educational areas, unless approved by the AISO.

### 49020.18.4 Operation of Computer Programs Created by Inmates

Any computer-based system that was created by inmate programmers that is used to accomplish or complete the CDCR-related work shall not be operated or maintained by any inmate.

### 49020.18.5 Supervision of Inmates Using Computers

The persons responsible for supervising inmates' use of computers shall certify in writing that these policies are being adhered to at their specific site.

A copy of this certification shall be kept on site by the local ISC.

### 49020.18.6 Education Computers

The use of computers for academic and vocational education is subject to the same requirement of due care applying to all personnel that use computers within applicability of the Department's information security and risk management program.

### 49020.18.7 PIA Systems

Inmate use of computers in PIA and in CDCR facilities shall be in accordance with the departmental policies and institutional procedures.

### 49020.19 Information Security-Warnings

All critical Department systems shall display a criticality warning at the first screen that any user of the system will see when the computer system is accessed.

### 49020.20 Revisions

The Director of EIS or designee shall be responsible for ensuring that the contents of this Article are kept current and accurate.

### 49020.21 References

The Constitution of the State of California, Article 1, Section 1.

The Information Practices Act of 1977, Civil Code § 1798.

The Federal Copyright Act of 1976.

The California Public Records Act.

Penal Code §§ 502, 11075-11081, 11142.

SAM, §§ 1601-1699, 5300-5360.1

GC §§ 1222, 6250-6265, 14740-14770.

DOM §§ Chapter 1, Article 23, and Chapter 4, Articles 31, 40, 41, 45, 46, 48.